CBSA PROTECTION • SERVICE • INTEGRITY

ASFC PROTECTION • SERVICE • INTÉGRITÉ

Biometrics Expansion Project

Privacy Impact Assessment (PIA)

Identity Management Unit
Traveller Transformation – Air Mode Division
Traveller Programs (Transformation) Directorate
Programs Branch

Ver. 2018-06-29

Version Control

Version	Author	Action	Date
1	Joanne, Percy, Katrina	Initial Draft	February 2018
2	Katrina, Percy	Review and comment	April 2018
3	Katrina, Joanne	Edits to Version 2	May 2018
	Katrina	Edits following consultation to Version 3	May 11 and June 3 2018
4		Review and submit to ATIP	
5		Revise to address ATIP feedback	
6		Revise to address ATIP feedback	
7		Revise to address ATIP feedback	
Final	Katrina	Copy for approval	June 29 2018

Stakeholders

Name	Role	Contact Information
Joanne Dolph	Program Officer	Joanne.Dolph@cbsa-asfc.gc.ca 343-291-5581
Percy Redhead	Senior Program Advisor	Percy.Redhead@cbsa-asfc.gc.ca 343-291-5605
Katrina Beecraft	Senior Policy, Planning and Performance Analyst	Katrina.Beecraft@cbsa-asfc.gc.ca 343-291-5582
Lori Pucar	Manager	Lori.Pucar@cbsa-asfc.gc.ca 343-291-5587
Robin Lortie	Manager, ATIP Policy and Governance	Robin.Lortie@cbsa-asfc.gc.ca 343-291-6987
Amy Cruickshank	Senior Policy Advisor, ATIP Policy and Governance	Amy.Cruickshank@cbsa-asfc.gc.ca 343-291-6983
Steve Whittaker	Manager, IT Risk Assessment and Consultation	Steve.Whittaker@cbsa-asfc.gc.ca 343-291-6936

Table of Contents

Privacy Impact Assessment Date / Version:	July 2018, Version 8
Office of the Privacy Commissioner file #:	
Project Implementation Plan (if applicable)	2018
Federal Institution:	Canada Border Services Agency (CBSA)
Related Class of Record Number:	Interdepartmental and Intergovernmental Relations Program CBSA ADM 132 Temporary Resident Biometrics Project (TRBP) CBSA IST 006
Personal Information Bank:	Traveller Processing CBSA PPU 1101 Temporary Resident Biometrics Program CBSA PPU 1203
Government Official Responsible for PIA:	Vice President, Programs Branch
Delegate for section 10 of the *Privacy Act*:	ATI and Privacy Director, Dan Proulx

EXECUTIVE SUMMARY

Immigration, Refugees and Citizenship Canada (IRCC) and the Canada Border Services Agency (CBSA) are jointly responsible for the delivery of Canada's immigration program by managing the movement of foreign nationals across Canada's borders in order to maintain a balance between the desire to welcome newcomers to Canada and the obligation to protect the health, safety, and security of Canadian society. Among the responsibilities of these departments are the prevention of irregular migration, the prevention of entry into Canada of inadmissible persons as defined by the *Immigration and Refugee Protection Act* (IRPA), and the detention and removal of inadmissible persons from Canada.

Accurately establishing identity is crucial to immigration decisions. For more than 20 years, biometrics (fingerprints and a photograph) have played a role in supporting immigration screening and decision-making in Canada.

Expanding biometrics will strengthen Canada's immigration programs through effective screening (biometric collection, verification, and information-sharing with partner countries). It will also enable Canada to facilitate application processing and travel – while maintaining public confidence in our immigration system.

In 2018-19, the CBSA will:

- Enroll certain foreign nationals applying for a work permit or study permit or temporary resident permit (excluding U.S. nationals) to enter Canada through the capture and screening of ten-digit fingerprint biometrics at fifty-seven Ports of Entry (POEs);
- Authenticate foreign nationals enrolled overseas by IRCC through a photo comparison and/or fingerprint verification upon arrival at POEs.

Depending on where they apply, applicants will be able to provide their biometrics in Canada at select Service Canada locations and select ports of entry, overseas at Visa Application Centres and in the U.S. at U.S. Application Support Centers.

Biometrics Expansion does not include collecting biometrics from Canadian citizens, citizenship applicants (including passport applicants), or existing permanent residents.

ABBREVIATIONS AND ACRONYMS

ATIP	Access to Information and Privacy
AUS	Australia
BAU	Biometrics Assessment Unit
BPO	Biometric Project Office
BOSU	Biometrics Operations Support Unit
BSO	Border Services Officer
CAIPS	Computer Assisted Immigration Processing System
CBSA	Canada Border Services Agency
COB	Country of Birth
COR	Class of Record
CCRTIS	Canadian Criminal Real Time Identification Services
CIBIDS	Canadian Immigration Biometrics Identification System (includes the biometric process solution and biometric collect solution)
CPIC	Canadian Police Information Centre
DOB	Date of Birth
DHS	Department of Homeland Security (U.S.)
DPA	Data Protection Authorities
DSO	Departmental Security Officer
EPIL	Electronic Primary Inspection Line
FA	Formal Arrangement
FPS	Fingerprint Section Number
GCMS	Global Case Management System
GOC	Government of Canada
GSP	Government of Canada Security Policy
HQ	Headquarters
HTTPS	Hypertext Transfer Protocol [Secure]
IBAS	Interdiction and Border Alert System
ICAO	International Civil Aviation Organization
IID	Immigration Identification
IIS	Immigration Information Sharing
IPIL	Integrated Primary Inspection Line
IRCC	Immigration, Refugees and Citizenship Canada
IRPA	*Immigration and Refugee Protection Act*

IRPR	*Immigration and Refugee Protection Regulations*
ISA	Information Sharing Agreement
IT/IM	Information Technology/Information Management
LAC	Library and Archives Canada
LSU	Legal Services Unit
M5	Migration Five (former Five Country Conference)
MOU	Memorandum of Understanding
MRZ	Machine Readable Zone
NZ	New Zealand
OGD	Other Government Department
OPC	Office of the Privacy Commissioner of Canada
PA	*Privacy Act*
PHAC	Public Health Agency of Canada
PAXIS	Passenger Information System
PDF	Portable Document Format
PI	Personal Information
PIA	Privacy Impact Assessment
PIB	Personal Information Bank
PIL	Primary Inspection Line
PKD	Public Key Directory
PNS	Privacy Notice Statement
PoE	Port of Entry
PR	Permanent Resident
RCMP	Royal Canadian Mounted Police
REP	Reasonable Expectation of Privacy
RFP	Request for Proposal
RTID	Real-Time Identification
SAR	Security Assessment Report
SOAP	Simple Object Access Protocol
SOR	System of Record
SOS	Statement of Sensitivity
SPPH	Secondary Processing and Passage History
SSC	Shared Services Canada
SOW	Statement of Work

SRE	Search Response
StatCan	Statistics Canada
TBS	Treasury Board Secretariat
TBIDS	Traveller Biometric Identity Database
TR	Temporary Resident
TLS	Transport Layer Security
TRA	Threat and Risk Assessment
TRBP	Temporary Resident Biometrics Program
TRV	Temporary Resident Visa
UCI	Unique Client Identifier
UK	United Kingdom
U.S.	United States
U.S. ASC	United States Applicant Support Centre
VAC	Visa Application Centre
VMS	Video Monitoring System
VP	Vice-President
VO	Visa Office
VPN	Virtual Private Network
WCA	Written Collaborative Arrangement

DEFINITIONS

Action Plan	The Action Plan describes the steps that the Program will take to address risks that have been identified by ATI and Privacy Division, Office of the Privacy Commissioner of Canada (OPC) and Treasury Board Secretariat (TBS).
Administrative purpose	The *Privacy Act* defines an "administrative purpose" to be the use of an individual's personal information in a decision-making process that directly affects that individual.
Consistent use	Is a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.
Data Matching	A comparison of personal data obtained from a variety of sources, including personal information banks, for the purpose of making decisions about the individuals to whom the data pertains. Data matching is a specialized activity involving the collection, use and disclosure of personal information that is subject to the various requirements of the *Privacy Act*.
Info Source	Is a series of annual TBS publications in which government institutions are required to describe their institutions, program responsibilities and information holdings, including PIBs and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the *Privacy Act*. Data-matching activities, use of the SIN and all activities for which privacy impact assessments were conducted have to be cited in *Info Source* PIBs, as applicable. The *Info Source* publications also provide contact information for government institutions as well as summaries of court cases and statistics on access requests.
Personal Information	Information about an identifiable individual as defined in section 3 of the *Privacy Act*. This definition, although lengthy, is not exhaustive, as indicated by the introductory phrase, "including, without restricting the generality of the foregoing". Information that is not specifically mentioned in the list may still be included in the definition of personal information if it qualifies as "information about an identifiable individual".
Personal Information Bank	Is a description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.
Privacy	The OPC describes "privacy" as *"... the right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses."*

SECTION 1 - OVERVIEW AND INITIATION

Report Objectives

This report is a Privacy Impact Assessment (PIA) for the Biometrics Expansion initiative. Biometrics Expansion is the evolution of the Temporary Resident Biometrics Program (TRBP) initiative for the Canada Border Services Agency (CBSA). This PIA should be considered in conjunction with the TRBP PIA which includes analysis on areas of technology and security which are unchanged for the Agency.

The objectives of this PIA are:

- To analyze the introduction of biometric collection at Ports of Entry (POE) in support of study permits, work permits and temporary resident permits for all nationalities (other than U.S.); and
- To analyze the expansion of biometric verification at POEs as it pertains to biometrically enrolled travellers seeking entry to Canada.

PIAs related to Immigration Information Sharing (IIS), TRBP and the Primary Inspection Kiosk (PIK) were provided to the Office of the Privacy Commissioner (OPC) and meetings were held to discuss the evolution of primary inspections at Canadian airports.

The information presented in this report follows the Treasury Board of Canada Secretariat (TBS) PIA policy and guidelines.

The purpose of the PIA process is to ensure that privacy is considered throughout the project development cycle. The results of a PIA are a documented guarantee that privacy issues have been identified and adequately addressed.

An Annex which includes the systems changes which support Biometrics Expansion has been included following the PIA.

Government Institution: CBSA / Programs Branch

Government Official Responsible for the Privacy Impact Assessment	Head of the government institution / Delegate for section 10 of the *Privacy Act*
Martin Bolduc, Vice President, Programs Branch	Dan Proulx, Director, Access to Information and Privacy Division

Name of Program or Activity of the Government Institution:

This initiative relates to the 1.3 Admissibility Determination sub-activity, 1.3.2 Air Mode sub-sub-activity and the 1.3.1 Highway Mode sub-activity.

Description of Program or Activity:

1.3 Admissibility Determination – through the Admissibility Determination program, the CBSA develops, maintains and administers the policies, regulations, procedures and partnerships that enable border services officers to intercept people and goods that are inadmissible to Canada, and to process admissible people and goods within established service standards. In addition, the Agency develops, maintains and administers the policies, regulations, procedures and partnerships to control the export of goods from Canada. In the traveller stream, border services officers question people upon arrival to determine if they and their personal goods meet the requirements of applicable legislation and regulations to enter Canada. Border services officers (BSOs) will then make a decision to grant entry or refer a person for further processing (e.g., payment of duties and taxes, issuance of a document), and/or for a physical examination.

1.3.1 Highway Mode - The Highway Program identifies and intercepts inadmissible people and goods seeking entry to Canada at 117 designated land ports of entry while ensuring that admissible people and goods are processed within established service standards. Border services officers conduct interviews of persons and drivers of commercial carriers and then make a decision to allow the entry of a person or shipment or refer them for further processing (e.g., payment of duties and taxes, issuance of a document) and/or examination (e.g., physical search of a vehicle, further investigation of admissibility).

In the commercial stream, importers are required to account for their goods, and carriers and exporters are required to report their goods.

Examinations may be performed with the use of specialized tools (e.g., gamma ray imaging Vehicle and Cargo Inspection System, ion scanners and detector dogs) and may include a full or partial offload of the goods to detect the presence of prohibited or restricted goods (e.g., narcotics or weapons). People and/or goods found to be in violation of the applicable legislation and/or regulations may be subject to a monetary penalty, seizure or denied entry to Canada.

1.3.2 Air Mode – The Air Program identifies and intercepts people and goods that are inadmissible to Canada seeking entry at designated airports while ensuring that admissible people and goods are processed within established service standards. Upon arrival, border services officers conduct interviews of persons seeking entry into Canada, aided by electronic pre-arrival risk-assessment information submitted by the airlines. CBSA officers make a decision to admit the person or refer them for further processing (e.g., payment of duties and taxes, issuance of a document) or examination. For private and corporate aircraft and general aviation traffic reporting through the Telephone Reporting Centre, various checks are conducted by means of the telephone reporting system. BSOs make a decision to admit people or refer them for further processing or examination. To assist border services officers in their examinations, detection tools such as detector dogs and ion scanners may be used. People and goods found to be in violation of the applicable legislation and/or regulations may be subject to a monetary penalty, seizure or denied entry to Canada.

Description of the class of records associated with the program or activity:

Biometrics Expansion (Bio) – Class of Records

Description: This class describes records related to applications made by clients at overseas offices and Canadian ports of entry (POE). The record will contain biographical data and a digital photograph of the applicant. The introduction of biometrics in the temporary resident stream screening process will enhance the admissibility screening of applicants, fix a client's identity at the time of application and allow the verification of that identity when this individual seeks entry at the border. The lead department on the project is Immigration, Refugees and Citizenship Canada (IRCC).

Note: It may include records related to the establishment or use of electronic systems used to administer or manage the program including; the Integrated Primary Inspection Line (IPIL), Integrated Customs Enforcement System (ICES), Secure Tracking System (STS), Screening Referral Request (SRR), Secondary Processing/Passage History (SPPH) and Global Case Management System (GCMS).

Document Types: Treasury Board Submission, Immigration and Refugee Protection Regulations, Project Charter, Concept of Operations.

Record Number: CBSA IST 006

Interdepartmental and Intergovernmental Relations Program

Description: Describes records relating to the Interdepartmental and Intergovernmental Relations Program which describes written information sharing collaborative agreements between the CBSA and federal departments. Records may also include Travellers Declaration cards, Casual Goods Accounting Documents, records or reports from electronic systems used to administer or manage the program including the GCMS, Travellers Entry Processing System (TEPS), the Customs Commercial System (CCS), the Facility for Information Retrieval Management (FIRM) and the Travellers National Database System (TRANDS).

Document Types: Memoranda of Understanding, Letters of Understanding, Information Sharing Agreements, Service Level Agreements, policy, guidance materials, Memos and Forms.

Record Number: CBSA ADM 132

Class of Record Number: CBSA IST 006 and CBSA ADM 132

☒ Proposal for a New Personal Information Bank
☐ Proposal to modify an existing Personal Information Bank - identify PIB registration number and current description:

Biometrics Program Personal Information Bank

Description:

This bank describes information that is used in support of the Biometrics Program. This includes applications for study, work or temporary resident permits from select nationalities at select ports of entry as well as biometric identity verification of enrolled travellers on entry to Canada. The personal information may include name, biometric information, citizenship status, date of birth, other identification numbers, physical attributes and place of birth.

Note:

Information may be stored in the following internal systems / databases: Traveller Biometric Identity Database (TBIS), the Global Case Management System (GCMS) (photo), Real Time Identification Database (RTID) (fingerprints), and Passage History (photo and fingerprint verification results).

Class of Individuals:

Travellers biometrically enrolled overseas, in Canada, or at a POE as part of the Biometrics Program.

Purpose:

The personal information is used to administer the biometrics program and to establish the identity of foreign nationals at a Canadian port of entry. Personal information is collected pursuant to sections 10.01 and 16 of

the *Immigration and Refugee Protection Act* and section 12.1 of the *Immigration and Refugee Protection Regulations*.

Consistent Uses:

The information may be used or disclosed for the following purposes: enforcement, reporting to senior management, security and identity management. Biographic and biometric information on foreign nations may also be shared with Regional Intelligence Officers / Intelligence Targeting Operations to assist in determining admissibility of travellers; refer to CBSA PPU 035.

PIA

Yes a PIA has been developed prior to the development of the PIB. The PIA was completed and submitted in July 2018.

Retention and Disposal Standards:

Records will be retained for 15 after from the time of the most recent biometric collection and will be systematically destroyed after 15 years or upon granting of Canadian citizenship. For persons deemed inadmissible under sections 34-37 of the *Immigration and Refugee Protection Act*, the fingerprints will be retained until the person reaches the age of 100 and then are destroyed.

RDA Number: 2015/008

Related Class of Record Number: CBSA IST 006, CBSA ADM 132

TBS Registration: TBD

Bank Number: CBSA PPU 1203

Legal Authority for Program or Activity:

Legal authority for the collection of biometrics is derived from the IRPA and subsequent IRPR.

The biometrics collection requirement includes all persons applying for a temporary or permanent resident visa or status, work permit, study permit, temporary resident permit, or refugee protection, whether claimed inside or outside Canada, unless specifically exempted.

Note: A person eligible to apply for an Electronic Travel Authorization (eTA) will not be required to provide their biometrics if they were travelling to Canada as a tourist.

Persons between the ages of 14 and 79 years applying for temporary or permanent residence are required to provide their biometrics. The Regulations specify that the age of the person will be determined as of the date on which the claim, application or request is made. The Regulations do not specify an upper age cut-off for those making a refugee claim in Canada for program integrity reasons.

The Regulations require a one-time biometrics enrolment from permanent residents when applying for a new permanent resident card if they were exempt from the biometrics collection requirement at the time they applied for permanent residence because they were under the age of 14 at the time of their application. Further, these applicants would not be issued a permanent resident card until they comply with the biometrics collection requirement.

The Regulations require that, where a person is required to provide their biometrics, they follow the prescribed procedures by presenting themselves at an enrolment facility located overseas, at a port of entry in Canada, or at other locations, if authorized or directed by an officer to do so.

Persons who are biometrically required and authorized to apply at a port of entry must present themselves at a port of entry that provides biometrics collection services. These persons would include

- Visa-exempt persons eligible to apply for a work or study permit at the port of entry; and
- Persons requesting and receiving a temporary resident permit.

The Regulations ensure that asylum claimants would continue to be able to make a claim for refugee protection at any port of entry.

Protected persons and Convention refugees who make an application for permanent residence from within Canada will be required to re-enrol their biometric information at a service location in Canada.

The Regulations specify that foreign nationals who make more than one temporary resident application (e.g. applications for both a work permit and study permit) before providing their biometric information will only need to provide their biometrics and pay the collection fee once.

Scope

This report will focus on two activities:

- The introduction of biometric collection at POEs in support of study permits, work permits and temporary resident permits for all nationalities (other than U.S.) and
  - Biometrics Enrolment in Secondary to be conducted at 57 POEs by BSOs (July 31 2018)
- The expansion of biometric verification at POEs as it pertains to biometrically enrolled travellers seeking entry to Canada
  - Systematic Fingerprint Verification at Primary Processing of enrolled applicants at POEs (CBSA) at ten major airports (Toronto, Ottawa, Vancouver, Montreal, Calgary, Edmonton, Halifax, Winnipeg, Quebec, Billy Bishop) through the PIK (March 2019)
  - Fingerprint Verification in Secondary to be conducted at 57 POEs by BSOs (July 31 2018)

Privacy considerations related to the collection and verification of biometrics have been addressed in other PIAs, including:

1. PIA for the Global VAC network (IRCC) (submitted in May 2017);
2. PIA for M5 information sharing regulations (CBSA) (submitted in June 2017);
3. PIA for U.S. service delivery channel (IRCC) (to be updated for June 2018);
4. PIA for in-Canada service delivery channel (IRCC) (to be updated for June 2018);
5. PIA related to collection and verification activities under the TRBP at POEs, including LiveScan (CBSA)(submitted in May 2014)
6. PIA for the Statement of Mutual Understanding of Information Sharing Citizenship and Immigration Canada (IRCC)(November 2002)
7. PIA for Case-By Case Immigration Information Sharing with the Migration Five (M5) Partners (referred to as IIS PIA) (CBSA) (submitted July 2016)
8. PIA related to the RTID system, including secondary use of information (RCMP)
9. PIA for Primary Inspection Kiosks (CBSA) (submitted in February 2017)

Summary of the Biometrics Expansion initiative:

Accurately establishing and managing identity is fundamental to the integrity of Canada's immigration programs and essential to ensuring the safety and security of Canadians. Biometrics provide a reliable and accurate means of validating and verifying identity while facilitating the entry of travellers for trade, commerce, study, tourism and other legitimate purposes that yield social and economic benefits to Canada.

Canada has been using biometrics to manage identity in the immigration program for over 20 years. Biometrics have been collected from asylum claimants since 1993, visa-required temporary residents from 30 nationalities since December 2013 and overseas refugee resettlement claimants since November 2014.

In 2013, Canada began biometric enrolment and screening for foreign nationals from 30 nationalities in support of their temporary resident visitor visa, work permit or study permit applications submitted overseas to IRCC under the TRBP. The TRBP introduced fingerprint verification by the CBSA at secondary examination on a discretionary basis at eight international airports.

In 2015, Canada and the U.S. began systematic biometric immigration information sharing where the fingerprints of all refugee protection claimants, overseas refugee resettlement applicants, and visa applicants subject to TRBP requirements are sent to the U.S., which will send back relevant immigration information on matches.

International partners are increasingly relying on biometrics as part of an effective migration control and security framework. However, Canada's biometric requirements apply to only 20% of the total visa-required population and currently there is limited authority and capacity to use biometrics upon arrival. These gaps leave Canada's immigration programs and border management vulnerable to identity fraud and prevent Canada from taking full advantage of the benefits that biometrics have to offer.

Biometrics Expansion will introduce new populations for biometrics collection and introduce new functionality in support of both facilitation and security, including:

- Expanding the current biometric screening and verification to all Temporary Resident Visa (TRV), work permit, study permit, and Temporary Resident Permit (TRP) applicants (excluding US nationals) and all Permanent Resident (PR) applicants—new populations;
- The introduction of automated systematic fingerprint verification of these travelers at primary inspection upon arrival at eight major airports (note, this service will be offered at ten airports; however, eight are in scope for the project)—new facilitation location and process;
- Expanding fingerprint verification at secondary examination to an additional 11 airports and 38 land POEs—new facilitation locations; and
- The introduction of biometric enrolment capacity to 11 air and 38 land POEs at secondary examination—new facilitation process.

Eligible Travellers

The expansion of the program sees the concepts from TRBP expanded to all temporary resident visa (TRV), study and temporary resident (TR) permit applicants (excluding U.S. citizens) and permanent resident (PR) applicants. While Biometrics is expanding to include new populations of travellers, the security, technology and privacy mitigation strategies outlined in the TBRP PIA are still applicable and continue to support this expansion.

The CBSA will only be biometrically enrolling study, work and temporary resident permit applicants at POEs. All PR applicants will be processed by IRCC and are outside of the scope of this PIA.

SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION

Type of Program or Activity	Level of Risk
Program or activity that does NOT involve a decision about an identifiable individual	☐ 1
Administration of Programs / Activity and Services	☒ 2
Compliance / Regulatory investigations and enforcement	☒ 3
Criminal investigation and enforcement / National Security	☒ 4

Details: The CBSA will collect biometric information from all visa-required persons, all persons applying for a work permit, study permit, temporary resident permit or temporary resident status (excluding United States nationals), and all permanent resident applicants. The CBSA will verify all biometrically enrolled travellers at Canada's major airports in primary using the PIK and expand fingerprint verification capacity in secondary at additional ports of entry (i.e. airports and land borders).

Biometric Enrolment: The CBSA will collect, using the LiveScan device in secondary, directly from the applicant, their biographical data and two biometrics - a digital photograph and 10 fingerprints. The photograph is sent to IRCC as part of the immigration enrolment. The fingerprints are sent to the RCMP RTID for a search of registered convictions and charges and biometric enrolment. Applicants at the POE are limited to: work, study and temporary resident permits, and under limited circumstances, applicants for permanent resident status in the overseas refugee resettlement category.

Biometric Verification in Secondary: The CBSA will verify, in secondary, the fingerprints of biometrically enrolled travellers referred for immigration purposes. A traveller may also be referred to secondary for fingerprint verification when identity cannot be established with certainty at Primary.

Biometric Verification in Primary: The CBSA will systematically verify, in primary, the fingerprints collected by IRCC or the CBSA during time of application using the PIK. This will allow the Agency to verify that the traveller presenting themselves at the PIK is a biometric match to the traveller who was issued a permit, visa or status. Further to this, a BSO may compare the photo collected during time of application to the live traveller.

Necessity

Biometrics screening will help facilitate the entry of travellers with legitimate identities by providing a reliable tool for identity management, both at the time of application and at the time of arrival at a port of entry. Biometrics screening also helps to keep Canadians safe. The collection and verification of biometrics, along with criminal and immigration screening and biometric-based information sharing, strengthen the integrity of Canada's immigration program. This helps prevent identity fraud, identify those who pose a security risk and stop known criminals from entering Canada. The verification of biometrics collected at the application stage permits a CBSA officer to confirm with absolute certainty that the traveller's identity is a match to their visa or permit.

Effectiveness

Biometrics expansion will permit the Government of Canada (GC) to close the gap identified in the immigration permit application process and in traveller processing. The use of biometrics will keep Canadians safe by ensuring that travellers are not entering Canada illegally. Additionally, it will provide BSOs with tools to identify known criminals and prevent their entry to Canada. The use of biometric algorithms to confirm identity is more effective than the visual inspection of a passport or digital photo. The use of fingerprint verification can be automated and will be used to mitigate border wait times in the air mode; verifying identity with absolute certainty will mitigate the need for lengthy immigration interviews currently being conducted by the CBSA.

Proportionality

In R. v. Simmons (1998), the Supreme Court of Canada recognized that there is a lowered expectation of privacy in the border context given the importance of effective border management has on the well-being of the nation. Further, the Ontario Court of Appeal reaffirmed the importance of effective border management in the R. v. Jones (2006) decision by recognizing Canada's control over its border "as a societal interest of sufficient importance to be characterized as a principle of fundamental justice" given that effective border management serves a number of crucial social interests that benefit the Canadian public.

Minimal Intrusiveness

The CBSA has examined less privacy-intrusive measures, including status quo and technological solution.

Status Quo- status quo (the TRBP, which includes 29 visa required countries and one territory to provide biometrics in support of their application) limits Canada's ability to verify the identity with absolute certainty as it is restrictive in membership. Expanding the GC's authorities to collect biometrics from this new population for verification at additional locations, and offering biometric enrolment at POE, provides the GC with a reliable and accurate means of validating and verifying identity while facilitating the entry of travellers for trade, commerce, study, tourism and other legitimate purposes that yield social and economic benefits to Canada.

Technological Solutions

Biometric Enrolment: The Agency currently has LiveScan devices deployed across the country. Biometrics Expansion introduces a new workflow called "Immigration" which will be used to conduct a biometric enrolment at POEs in support of permit applications.

Biometric Verification in Secondary: The Agency currently has multiple verification devices deployed across the country. Biometrics Expansion introduces new work locations, all in secondary processing, where fingerprint verification will be available.

Biometric Verification in Primary: The CBSA will systematically verify, in primary, the fingerprints collected by IRCC or the CBSA during time of application using the PIK. The PIKs are existing kiosks; the verification devices are new technology which will be procured by Airport Authorities.

Type of Personal Information Involved and Context	Level of Risk
Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program.	☐ 1

Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.	☒ 2
Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual.	☒ 3
Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.	☒ 4

Details:

Biometric Enrolment: Biographical information and biometrics are provided directly by the traveller, by scanning their travel document, having their live photograph captured and by having their fingerprints captured. All of this information is captured in the LiveScan device using the "Immigration" workflow and sent to IRCC and the RCMP (fingerprints only). Specific elements of Biographic Data Entry include: Name, Alias, Sex, Date of Birth and Country of Birth. Specific Biometric Data Elements include: Digital photograph is sent to IRCC; fingerprints are captured and are sent to the RCMP and a one-to-many search is conducted in RTID.

Biometric Verification in Secondary: Fingerprints are captured using the certified fingerprint verification device and securely transmitted to the RCMP for a 1 to 1 verification in RTID.

Biometric Verification in Primary: Fingerprints are captured using the certified fingerprint verification device and securely transmitted to the RCMP for a 1 to 1 verification in RTID.

Program or Activity Partners and Private Sector Involvement	Level of Risk
Within the CBSA (amongst one or more programs within the CBSA)	☒ 1
With other federal institutions	☒ 2
With other or a combination of federal/ provincial and/or municipal government(s)	☐ 3
Private sector organizations or international organizations or foreign governments	☐ 4

Details: Primary and secondary processing is completed by CBSA officials. This occurs on-site at Canadian airports and land ports of entry. A Service Level Agreement (SLA) was signed with the RCMP which governs the relationship between the CBSA and the RCMP as it pertains to the RTID database and service standards. All biometrics collected by the Agency are encrypted and adhere to both CBSA and RCMP information management and information security requirements. All biometric collection devices (both enrolment and verification) are certified for use by the RCMP.
As stated in the PIK PIA, at no time will the Airport Authorities have access to the information collected by the CBSA.
The infrastructure for the data exchange is provided by Shared Services Canada (SSC). At no time will SSC have access to the information collected by the CBSA.

Duration of the Program or Activity	Level of risk
One time program or activity Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.	☐ 1
Short–term program A program or activity that supports a short-term goal with an established "sunset" date.	☐ 2
Long-term program Existing program that has been modified or is established with no clear "sunset".	☒ 3

Details: The expansion of biometrics collection is a priority for the GC; it was announced in the 2015 *Budget Implementation Act* (BIA) and subsequent regulations through pre-publication in the Canada Gazette Volume I.

Implementation of the project will automate administrative tasks, freeing up CBSA officers to focus on judgement-based decision-making and enforcement activities at the POE. Canada's reputation as a leader in border security will be strengthened as the Agency continues to prevent immigration fraud and illegal entry to Canada.

Program Population	Level of Risk
The program affects certain employees for internal administrative purposes.	☐ 1
The program affects all employees for internal administrative purposes.	☐ 2
The program affects certain individuals for external administrative purposes.	☒ 3
The program affects all individuals for external administrative purposes.	☐ 4

Details: This project affects all visa-required persons, all persons applying for a work permit, study permit, temporary resident permit or temporary resident status (excluding United States nationals), and all permanent resident applicants.

Technology and Privacy	
6.1 Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information?	☒ YES ☐ NO
6.2. Does the new or modified program or activity require any modifications to IT legacy systems and / or services?	☒ YES ☐ NO
6.3 Does the new or modified program or activity involve the implementation of one or more of the following technologies:	
6.3.1 Enhanced identification methods: This includes biometric technology (i.e. facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID), etc...) as well as easy pass technology, new identification cards including magnetic stripe cards, "smart cards" (i.e. identification cards that are embedded with either an antenna or a contact pad that	☒ YES ☐ NO

is connected to a microprocessor and a memory chip or only a memory chip with non-programmable logic).	
6.3.2 Use of Surveillance: This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance / interception, computer aided monitoring including audit trails, satellite surveillance etc.	☐ YES ☒ NO
6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques: For the purposes of the Directive on PIA, CBSA is to identify those activities that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence and/or machine learning to uncover knowledge (intelligence), trends/patterns or to predict behaviour.	☒ YES ☐ NO

Details: The technological solutions for enrolment and verification are not new to the Agency.

Biometric Enrolment: The CBSA will collect, using the LiveScan device in secondary, directly from the applicant, their biographical data and two biometrics- a digital photograph and 10 fingerprints. The LiveScan device is not new; however, a new workflow, specifically for immigration enrolment under biometrics expansion has been added to the device core. The elements collected were described previously in this PIA. For the purposes of the Biometrics Expansion Project, additional LiveScan devices have been added at new work locations.

Biometric Verification in Secondary: As outlined in the TRBP PIA the CBSA will continue to verify, in secondary, the fingerprints of biometrically enrolled travellers. For the purposes of the Biometrics Expansion Project, additional verification devices have been added at new work locations.

Biometric Verification in Primary: The CBSA will systematically verify, in primary, the fingerprints collected by IRCC or the CBSA during time of application using the PIK.

Personal Information Transmission	Level of Risk
The personal information is used within a closed system. No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.	☒ 1
The personal information is used in system that has connections to at least one other system.	☒ 2
The personal information is transferred to a portable device or is printed. USB key, CD-ROM, laptop computer, any transfer of the personal information to a different medium.	☒ 3
The personal information is transmitted using wireless technologies.	☐ 4

Details: All personal information and biometrics will be used within a closed system which has connections to at least one other system. Information will not be transferred to any portable devices, however, the printing of forms is permissible.

Biometric Enrolment: The CBSA official can print forms associated with the application; however, this would not be standard practice. Should an officer decided to print a non-mandatory form, the form would be stored in accordance with the Agency's security and record retention policies.

Biometric Verification in Secondary/Primary: There is no printing of information concerning fingerprint verification results. The verification results from the RCMP will not be included in the PIK receipt.

Risk Impact to the CBSA	Level of Risk
Managerial harm. Processes must be reviewed, tools must be changed, change in provider / partner.	☐ 1
Organizational harm. Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.	☐ 2
Financial harm. Lawsuit, additional moneys required reallocation of financial resources.	☐ 3
Reputation harm, embarrassment, loss of credibility. Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the GC Outcome areas.	☒ 4

Details: In the event of a breach of the personal information collected and transmitted by the Agency, there would be a decrease in public confidence regarding the CBSA's ability to responsibly handle personal information. Given the safeguards in place this is unlikely. A Critical Security Assessment Report (CSAR) has been conducted by CBSA IT Security; it will be finalized in advance of Coming-Into-Force of the project. Preliminary assessments show no indication of any security issues which would prevent the project from moving forward as planned.

Risk Impact to the Individual or Employee	Level of Risk
Inconvenience.	☒ 1
Reputation harm, embarrassment.	☒ 2
Financial harm.	☒ 3
Physical harm.	☐ 4

Details: In the event of a breach of personal information collected and transmitted by the CBSA, there could be the possibility of identity theft for the individual. Again, the Service Level Agreement, initiative design, systems architecture and configuration requirements provide an adequate level of protection to mitigate this risk. Personal data is stored in multiple locations (systems) and using a variety of security measures. A security breach would not reveal an entire biometric collection file as it pertains to an individual applicant.

SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS

Personal Information Bank – Biometrics Expansion Program

Biometric Enrolment

The following table lists the personal information elements collected, used, disclosed and retained via the biometric enrolment information flow.

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Source	Purpose / Necessity of Element
Biographic Information	Name	Last name First name Middle initial	Electronic	Derived from the client's passport	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
	Date of birth	Day of birth Month of birth Year of birth	Electronic	Derived from the client's passport	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
	Gender	Male/Female/Gender X	Electronic	Derived from the client's passport	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
	Place of birth		Electronic	Derived from the client's passport	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
	Citizenship		Electronic	Derived from the client's passport	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
Passport/Travel Document Information	Passport/Travel Document Information		Electronic	Derived during the application process	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
Biometric Information	Fingerprints	Fingerprints Location fingerprints collected Date Authority to collect Age	Electronic	Direct collection of fingerprints at POE	To fix the applicant's biometric identity, authenticate identity and determine admissibility through a one to many query of the RID database.

Biometric information	Digital Photograph	Digital Photograph	Electronic	Direct collection of photograph at POE	To compare photograph with the photograph on the passport submitted in support of application. In future, this photograph will allow the CBSA to confirm identity as it pertains to the permit application.
Fingerprints & related biographical data sent to the RCMP	Fingerprints only and Immigration ID Number—IID	Fingerprints and Immigration ID Number—IID	Electronic	CBSA	Data to enable accurate storage and/or to be used for a one to one identity verification.
Fingerprint Assessment Results from RCMP	Fingerprint Assessment Results	Response sent to CBSA from RCMP following one-to-one verification: • Match; **or** • No match; **or** • Unable to certify (low quality prints); **or** • File number not found (i.e., IID number)	Electronic	RCMP **generated by RCMP systems	To establish biometric identity, authenticate identity and determine whether applicants meet admissibility requirements under *IRPA* at time of application and at POE.
Information sent to CBSA once a positive decision is rendered on an application by IRCC		A copy of the applicant's photograph and tombstone data Document Number Fingerprint indicator The results of the fingerprint search and the assessment	Electronic	IRCC **partially collected from applicant or generated by RCMP systems and IRCC processing officers	To establish biometric identity, authenticate identity and determine whether applicants meet admissibility requirements under *IRPA* at time of application and at POE.

Biometric Verification at Secondary

The following table lists the personal information elements collected, used, disclosed and retained via the verification at secondary information flow.

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Source	Purpose / Necessity of Element
Biographic Information	Name	Last name First name Middle initial	Electronic	Derived from the client's passport	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
	Date of birth	Day of birth Month of birth Year of birth	Electronic	Derived from the client's passport	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.

	Gender	Male/Female/Gender X	Electronic	Derived from the client's passport	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
	Place of birth		Electronic	Derived from the client's passport	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
	Citizenship		Electronic	Derived from the client's passport	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
Passport/Travel Document Information	Passport/Travel Document Information		Electronic	Derived during the application process	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
Biometric information	Fingerprints	Fingerprints Location/Date/Reason for Fingerprints years of age and older.)	Electronic	Direct collection of fingerprints at POE for verification	To fix the applicant's biometric identity, authenticate identity and determine admissibility through: one to one RTID verification match of an applicant who has previously submitted fingerprints under the application process and arrives at a POE.
Biometric information	Digital Photograph	Digital Photograph	Electronic	Indirect collection of photograph collected from IRCC or CBSA	Where fingerprints are not being used to confirm identity as it pertains to the permit or Visa application.
Fingerprints & related biographical data sent to the RCMP	Fingerprints only and Immigration ID Number—IID	Fingerprints and Immigration ID Number—IID	Electronic	CBSA	Data to accompany fingerprints for conduct of verification match to support determination of admissibility under IRPA.
Fingerprint Assessment Results from RCMP	Fingerprint Assessment Results	Response sent to CBSA from RCMP following one-to-one verification: • Match; **or** • No match; **or** • Unable to certify (low quality prints); **or** • File number not found (i.e., IID number)	Electronic	RCMP **generated by RCMP systems	To establish biometric identity, authenticate identity and determine whether applicants meet admissibility requirements under *IRPA* at time of application and at POE.
Information sent to CBSA once a positive decision is rendered on an application by IRCC		A copy of the applicant's photograph and tombstone data Document Number Fingerprint indicator The results of the fingerprint search and the assessment	Electronic	IRCC **partially collected from applicant or generated by RCMP systems and IRCC processing officers	To establish biometric identity, authenticate identity and determine whether applicants meet admissibility requirements under IRPA at time of application and at POE.

Biometric Verification at PIK

The following table lists the personal information elements collected, used, disclosed and retained via the verification at PIK information flow.

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Source	Purpose / Necessity of Element
Biographic Information	Name	Last name First name Middle initials	Electronic	Derived from the travel document at the kiosk	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
	Date of birth	Day of birth Month of birth Year of birth	Electronic	Derived from the travel document	To identify travellers in existing CBSA information holdings and assess admissibility.
	Gender	Male/Female/Gender X	Electronic	Derived from the travel document	To identify travellers in existing CBSA information holdings and assess admissibility.
Province/Country Information	Partial Address	Country Province (for residents of Canada) State (for residents of the U.S.)	Electronic	Traveller data entry at kiosk	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility. Place of residence is also used to determine which additional customs related questions are asked to a traveller (i.e., defines resident vs. non-resident).
Biometric	Visual Image	Visual image of the traveller, taken by the kiosk. (Note: visual images are only captured for travellers that are 14 years of age and older.)	Electronic	Photo capture at the kiosk	To authenticate that the client in front of the kiosk corresponds with the individual's photo embedded in the chip of their ePassport chip (for the clients that have this feature in their passport). For all clients, the photo will be printed on the kiosk receipt as a means of connecting the individual(s) with their declaration throughout the rest of the CBSA service area. CBSA officers will manually authenticate that the individual(s) presenting the receipt are those featured in the photos. This will improve traveller flow, strengthen travellers' identity reconciliation, and limit internal conspiracy issues such as receipt / declaration swapping by individuals trying to circumvent referral to and examination at Secondary.
Citizenship / Nationality	Citizenship / Nationality	Citizenship / nationality of traveller	Electronic	Derived from the travel document at the kiosk	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
Purpose of Trip	Purpose of trip	Personal Study Work or Employment Immigrate	Electronic	Traveller data entry at kiosk	To assess admissibility of foreign national travellers.

Travel Document Information (may be their Passport)	Travel Document Information	Document Type Document Number Document Country of Issuance Document expiration date Public Key Directory (PKD)	Electronic	Derived from the travel document	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility; to verify the validity and authentication of the travel document. In the past, a CBSA officer would manually verify the travel document; through PIK, the kiosk will conduct these tasks, validating the document against PKD information.
Biometric information	Fingerprints	Fingerprints	Electronic	Direct collection of fingerprints at POE for verification	To fix the applicant's biometric identity, authenticate identity and determine admissibility through: one to one RTID verification match of an applicant who has previously submitted fingerprints under the application process and arrives at a POE. *This is the only new element introduced through the Biometrics Expansion Project
Fingerprint Assessment Results from RCMP	Fingerprint Assessment Results	Response sent to CBSA from RCMP following one-to-one verification: • Match; **or** • No match; **or** • Unable to certify (low quality prints); **or** • File number not found (i.e., IID number)	Electronic	RCMP **generated by RCMP systems	To establish biometric identity, authenticate identity and determine whether applicants meet admissibility requirements under *IRPA* at time of application and at POE. Note, the fingerprint assessment response from the RCMP is never, under any circumstance, communicated to the traveller by the PIK.
Customs and OGD Related Questions	Declaration questions	Declaration questions related to: 1) Firearms or other weapons 2) Commercial goods 3) Food, plant or animals 4) Currency (more than $10,000) 5) Unaccompanied goods 6) Visit to a farm abroad and destined to a farm in Canada Declaration related to personal exemption (returning residents) and allowance (visitors); and value of goods for travellers indicating they exceeded their exemption limit.	Electronic	Traveller data entry at kiosk	To assess duties and taxes; to assess goods admissibility.
Duration of stay in Canada	Duration of stay in Canada	Duration of stay in Canada	Electronic	Traveller data entry at kiosk	To assess admissibility of foreign national travellers.

Duration of stay outside of Canada	Duration of stay outside of Canada	Duration of absence from Canada	Electronic	Traveller data entry at kiosk	To assess traveller exemption allowance for Canadian residents
Signature	Electronic Signature	Physical signature replaced by on-screen confirmation that the declaration is true, accurate and complete.	Electronic	Traveller data entry at kiosk	Validation of the information provided.

SECTION 4 - FLOW OF PERSONAL INFORMATION

4.1 Data Flow Model - Diagram

Diagram 1 – Biometric Enrolment at Secondary

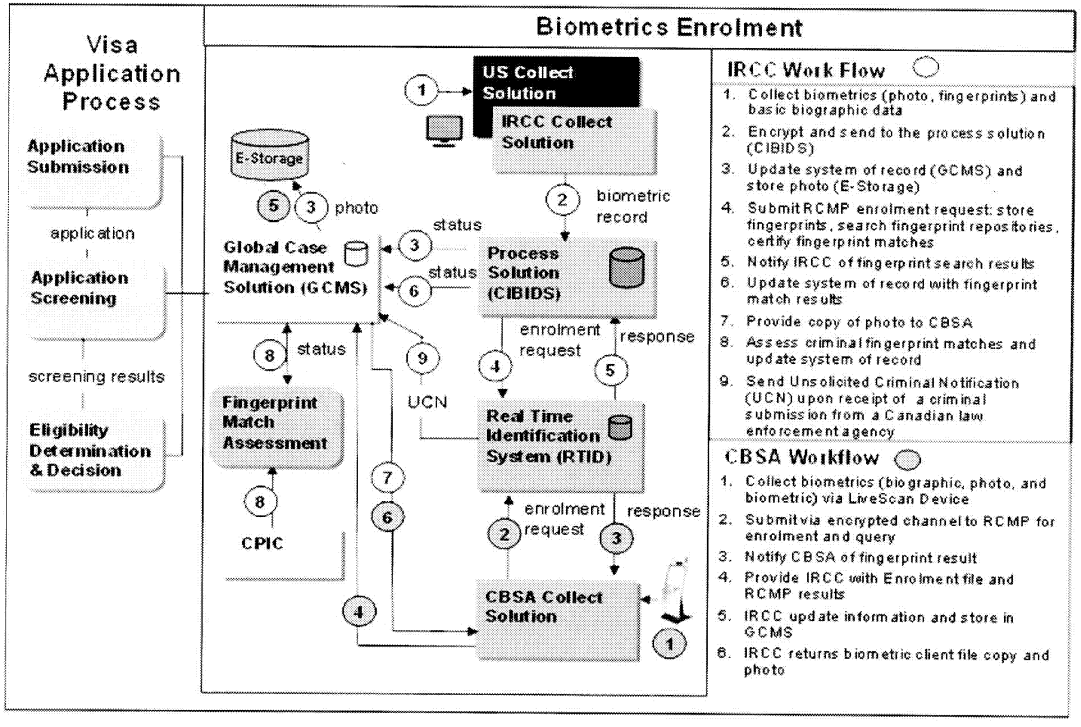
Start: A traveller who is eligible makes an application at a POE for a study or work permit or requires a TRP to overcome their inadmissibility.

In all automated POEs, select information received from GCMS will be available to CBSA BSOs at the primary inspection (PIL) line in order to make an admissibility decision. The CBSA BSOs may make a visual comparison of the applicant and the passport photograph to make decisions about entry into Canada. If the traveller is admissible but requires a study or work permit, they will be referred to secondary for biometric enrolment. If the traveller is inadmissible to Canada but may overcome their inadmissibility through a TRP, they will be referred to secondary for biometric enrolment. The decision that the traveller is eligible is based on the following elements:

- A copy of the applicant's photograph and tombstone data as presented in their travel document

Once in the Secondary Examination Area the traveller will have their fingerprints and photo taken as part of their biometric enrolment. These fingerprints, will be sent directly from CBSA to the RCMP for a one-to-many query against the RTID fingerprint database held by the RCMP.

- The BSO will open the application in GCMS and can then begin biometrics collection.
  1. The traveler will begin enrolment at the LiveScan device which will capture select biographic fields which are auto-populated from GCMS in addition to the traveller's digital photograph and 10 fingerprints.



2. Once the biometric data is collected, it will be securely transmitted to the process solution. The fingerprints and the associated biographical data will be subsequently forwarded to the RCMP RTID system via a secure transmission.
3. The RCMP will conduct a search in the RCMP RTID system against records of previous deportees, refugee claimants, previous TR/PR applicants and criminal records (Canadian or foreign records held by the RCMP in the RTID Criminal Data Base) to determine if there are any matches to the collected fingerprints. The RCMP RTID system will store the digital fingerprints and associated biographical data received and then perform a search in the RTID system. The RCMP RTID system will return a response to the CBSA LiveScan device.
4. GCMS will populate the biographical data sent by the process solution.
5. The digital photograph however will only be forwarded to CBSA's e-storage once the BSO renders a decision on the traveller's application, where it will be available for future use by CBSA and IRCC. See Verification Diagram for more information on e-storage.
6. The LiveScan device will receive an SRE from the RCMP RTID system and relay the information to GCMS through Canadian Immigration Biometric Identification Systems (CBIDS).

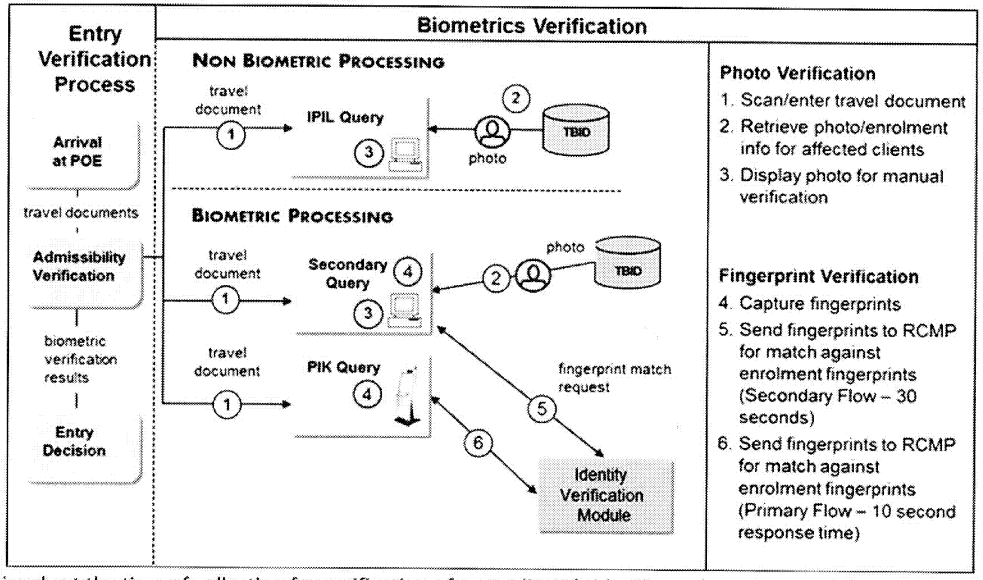
The LiveScan will also record and transmit event logs to the process solution relating to each collection activity (e.g., log-ins, sessions opened, sessions cancelled, data captured, etc.), where they will be made available for oversight, reporting and monitoring purposes by CBSA.

The BSO makes final decision at POE based on the applicant's biometric data, the results from the RCMP as well as any other required documents and/or available data. At any point in the enrolment process, there are no fingerprints stored electronically by the CBSA. If an error message is received from the RCMP about the transmission of fingerprints, the BSO will troubleshoot the error.

The regulations include a discretionary authority for CBSA officers to exempt the biometric enrolment requirement for travellers in exceptional circumstances (i.e. system outage, urgent need, etc.) when the officer is confident in the applicant's identity. In such cases the BSO will revert to existing procedures to make the admissibility determination and the traveller will be biometrically enrolled at the next encounter (if biometric enrolment is still required).

Diagram 2 – Biometric Verification in Primary and Secondary

Start: Registration of the applicant's biographical information via scanning the Machine Readable Zone (MRZ) information strip on a passport or travel document (or manually entering the biographical data if an MRZ travel document is not available).
Traveller Processing CBSA PPU 1101
Temporary Resident Biometrics Program CBSA PPU 1203

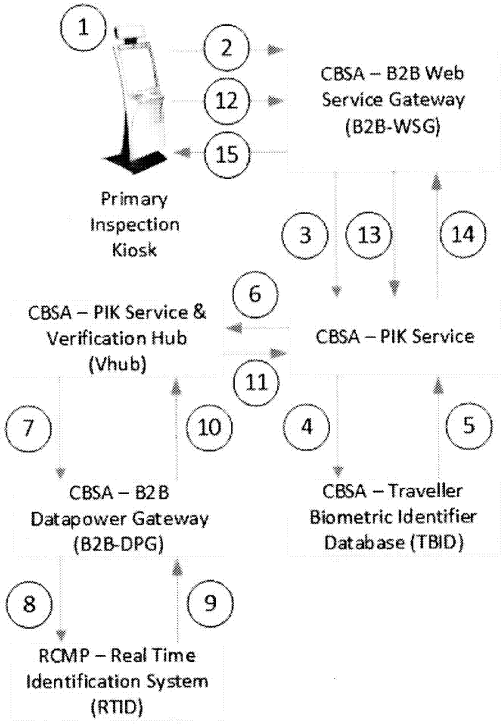


1. At the Primary Inspection Line (PIL) in all automated POEs, select information received from IPIL will be available to CBSA BSOs in order to make an admissibility decision.
2. IPIL sends a request to TBID to retrieve the biometric photo.
3. The CBSA BSOs may make a visual comparison of the applicant and the passport photograph with the photograph from TBID (displayed in the Secondary Query, SPPH) to make decisions regarding entry into Canada.
4. At PIK enabled POEs biometrically enrolled travellers will be prompted to have their fingerprints taken for the purposes of identity verification. At both PIK and non-PIK POEs, biometrically enrolled travellers may be referred to a Secondary Examination Area based on an inconclusive admissibility. decision or for other immigration processing or admissibility purposes. Once in the Secondary Examination Area the traveller may have their fingerprints taken as part of their admissibility assessment portion of the examination.
5. The SPPH system will send these fingerprints, along with their IID, directly from CBSA to the RCMP for a 1:1 verification process against the fingerprints the applicant previously provided at the time of collection. Upon receiving the fingerprints from CBSA, the RTID system will verify them against those taken previously at the time of collection for verification of an applicant's identity and provide a match, no match or unable to auto certify response (i.e., 1:1 match)[2]
6. The PIK sends these fingerprints, along with their IID, directly from CBSA to the RCMP for a 1:1 verification process against the fingerprints the applicant previously provided at the time of collection. Upon receiving the fingerprints from CBSA, the RTID system will verify them against those taken previously at the time of collection for verification of an applicant's identity and provide a match, no match or unable to auto certify response (i.e., 1:1 match). The PIK service will then use the fingerprint verification result to inform a release (grant entry) or referral decision based on the PIK referral logic matrix.

The BSO makes a final decision at POE based on the applicant's biometric data, the results from the RCMP as well as any other required documents and/or available data. At any point in the verification process, there are no fingerprints stored by CBSA. If an error message is received from the RCMP about the transmission of fingerprints, the BSO will use existing tools to verify identity or where possible, will troubleshoot the error.

In the event that the verification equipment and/or system is malfunctioning, the BSO will revert to existing procedures to make the admissibility determination (Non Biometric Processing).

Diagram 3 – Biometric Verification in Primary at a PIK (detailed)



Start: A traveller makes an application at PIL for entry to Canada using a PIK by presenting their travel document. If an IID is on-file and the traveller is biometrically enrolled, the kiosk will prompt the traveller for fingerprint verification.

1. Collect biometrics (biographic, photo, and fingerprint biometric) via PIK device.
2. Kiosk submits encrypted fingerprint (NIST) package to CBSA over secure channel to the B2B Web Service Gateway (B2B-WSG).
3. CBSA Web Service Gateway forwards the request to the CBSA PIK Service.
4. CBSA PIK Service retrieves the unique ID (IID) for previously enrolled traveller stored in the TBID database.
5. TBID returns the unique identifier for the biometrically enrolled traveller to the PIK Service.
6. CBSA PIK Service invokes the Biometric Verification Hub (VHub) with the NIST package and IID.
7. VHub enhances the NIST package with the CBSA agency identifiers and makes a request to the B2B Datapower Gateway service to invoke the RCMP query.
8. CBSA B2B-DPG submits NIST package via encrypted channel to RCMP for 1:1 verification.
9. RCMP will respond to the CBSA B2B-DPG over the encrypted channel to provide the verification search results to the CBSA.
10. The CBSA B2B-DPG will provide the RCMP results back to the VHub service.
11. The VHub service will deliver the RCMP results to the PIK Service where the results will be stored in anticipation of a completed session at the Kiosk.
12. When the traveller completes their Kiosk session, the declaration will be sent to the CBSA B2B-WSG.
13. The CBSA B2B-WSG will deliver the verified request to the PIK Service.
14. The CBSA PIK Service will process the declaration, and factor the RCMP results into the referral logic and create an immigration referral if a non-match, inconclusive, or technical error is encountered. The PIK Service will deliver the PIK Receipt back to the B2B-WSG.
15. The CBSA B2B-WSG delivers the PIK Receipt to the Kiosk, where it will be printed and the Traveller can collect it and present it to the Podium Officer who may direct to Referral Officer, Secondary Officer, or release the traveller.

The BSO makes a final decision at POE based on the applicant's biometric data, the results from the RCMP as well as any other required documents and/or available data. At any point in the verification process, there are no fingerprints stored by CBSA or by the PIK. There are no fingerprint verification results printed on the PIK receipt. If an error message is received from the RCMP about the transmission of fingerprints, the BSO will use existing tools to identify identity or where possible, will troubleshoot the error.

In the event that the PIK is malfunctioning, the BSO will revert to existing Primary Processing procedures to make the admissibility determination; biometric processing would remain available in Secondary Examination.

4.2 Data Flow Model - Table

SOURCE	IDENTIFY THE SOURCE
The individual or a representative	Traveller
CBSA Information Holdings	CBSA Information holdings such as: • Integrated Customs System (ICS): A common platform for managing authorized and authenticated access to the CBSA systems: o PIK Service - that handles the orchestration and coordination of primary processing for each traveller using the self-service Kiosk option. o Secondary Processing and Passage History (SPPH) to store traveller encounters, including declaration data, referral codes, previous fingerprint verification results, and examination results. o Passenger Information System (PAXIS) to retrieve passenger and flight information through the Advance Passenger Information (API) – CBSA PPU 008. • Integrated Custom Enforcement System (ICES) – CBSA PPU 016. Data from the following programs is accessed through ICES: o Criminal Investigation Program – CBSA PPU 1402; and o Intelligence Program – CBSA PPU 035. • Interdiction and Border Alert System (IBAS). Data from the following programs/systems is retrieved through IBAS: o Immigration Investigations Program – CBSA PPU 1403 o Enforcement Information Index System (EIIS) – CBSA PPU 025 o Document Integrity Program – CBSA PPU 1404 The Lost Stolen Fraudulent Document (LSFD). *Immigration related data is retrieved from Global Case Management System (GCMS) through IBAS.
Royal Canadian Mounted Police Information Holdings	A subset of Wants and Warrants from Canadian Police Information Centre (CPIC) is sent to ICES (CBSA PPU 016).

4.3 Internal Use and Disclosure

Program	Personal information bank
Secondary Processing	Traveller Processing PIB - CBSA PPU 1101

4.4 External Use and Disclosure

The individual or a representative	
A federal government institution	IRCC, as per the terms of the PIBs • Visitor Case File: CIC PPU 055 • Foreign Student Records and Case File: CIC PPU 051 • Temporary Worker Records and Case File: CIC PPU 054 • Overseas Immigration Case Files: CIC PPU 039
Non-federal institutions and private sector	
- Provincial Government	No systematic disclosures; any disclosures would be pursuant to Section 8(2) of the *Privacy Act* and/or Section 107 of the *Customs Act*
- Municipal Government	No systematic disclosures; any disclosures would be pursuant to 8(2) of the *Privacy Act* and/or Section 107 of the *Customs Act*
- Aboriginal Government / Council	No systematic disclosures; any disclosures would be pursuant to 8(2) of the *Privacy Act* and/or Section 107 of the *Customs Act*
- Organization of a Foreign State	M5 Partner (U.S., U.K., AUS, and NZ)
- International Organization	No systematic disclosures; any disclosures would be pursuant to 8(2) of the *Privacy Act* and/or Section 107 of the *Customs Act*
Private Sector	
- Located in Canada and Canadian Owned	None
- Located in Canada and Foreign Owned	None
- Located abroad and Canadian Owned	None
- Located abroad and Foreign Owned	None

The following section examines privacy compliance (at a high level) for the transparency of the disclosure of information, as included in this project The disclosure of information to any other government departments, per existing agreements, is not further explored in this PIA, as there are no changes to the established processes.

4.5 Retention / Storage

A federal government institution	RCMP IRCC CBSA
A Federal Records Centre	N/A
Non-federal institutions and private sector	
- Provincial Government	N/A
- Municipal Government	N/A
- Aboriginal Government / Council	N/A
- Organization of a Foreign State	N/A
- International Organization	N/A
Private Sector	
- Located in Canada and Canadian Owned	N/A
- Located in Canada and Foreign Owned	N/A
- Located abroad and Canadian Owned	N/A
- Located abroad and Foreign Owned	N/A

4.6 Other Possible Considerations

Identify Groups or Areas / or Divisions	Positions who have access or use the personal information (where appropriate)	Geographical Location
The CBSA responsible for program or activity:		
CBSA Programs	Approximately 25-50 staff members	National Capital Region
CBSA Information, Science and Technology	Approximately 20-25 staff members in a production support role, responsible for receiving incidents and requests from end-users, analyzing these and either responding to the end user with a solution or escalating it to the other IT teams. These teams may include developers, system engineers and database administrators handling system issues	National Capital Region
CBSA Operations	Approximately 4500 staff members including Border Services Officers,	All Ports of Entry

	interns/students, Superintendents, Chiefs of Operations	
CBSA Recourse	Approximately 25-30 staff members handling recourse and appeals	National Capital Region and Regional Offices
Other federal government Institution responsible for program or activity:		
Statistics Canada	StatCan estimates access is limited to 50 staff members, including scanning clerks and statisticians. No biometric information is shared	National Capital Region

SECTION 5 - PRIVACY COMPLIANCE ANALYSIS

1. Legal Authority for Collection of Personal Information

Has a legal authority been identified for the collection of personal information for this program or activity?

Yes

1.1 ☒ Specify the legal authority and briefly explain its connection to the program or activity or how it permits the collection of the personal information:

Legal authority for the collection of biometrics (digital photograph and fingerprints) is derived from the *Immigration and Refugee Protection Regulations (IRPR).*

Yes

1.2 ☒ Is the personal information collected directly related to an operating program or activity?

Details: The information collected has been cross-referenced with the purpose of collection.

No

1.3 ☐ If there is no legal authority for the collection of personal information, it cannot be collected. Please consult your legal advisor to determine if there is authority to proceed with the program or activity.

2. Necessity to Collect Personal Information

Is each element and sub-element of personal information collected or to be collected necessary to administer the program or activity?

YES

2.1 ☒ Ensure that all personal information necessary to administer the program or activity is listed in the relevant **PIB.**

2.2 ☒ AND, implement controls and procedures to ensure the CBSA does not collect more personal information than is necessary for the identified program or activity and that a continuing need exists for that information or its collection.

2.3 Are secondary uses contemplated for the information collected?

☒ YES ☐ NO

The use of the information for enforcement (if required) internal to the CBSA and disclosures to other government departments such as StatsCan would be considered secondary uses. These uses are documented in the Personal Information Bank and notice is provided to the individual at the point of collection through a Privacy Notice at the PIK and at time of enrolment at the LiveScan device.

2.3.2 If not, is there authority for the use or disclosure of the personal information?

☒ YES ☐ NO

NO

2.3 ☐ Review the proposed elements and sub-elements of personal information outlined in *"Section 3 – Analysis of Personal Information Elements"* to identify those that are "necessary" and not merely useful. Document any changes.

3. Authority for the Collection, Use or Disclosure of the Social Insurance Number

Is the collection of the Social Insurance Number (SIN) necessary to administer the program or activity?

YES

3.1 ☐ Collection of the SIN must be in compliance with the *Directive on Social Insurance Number (*please check all appropriate boxes below):

3.2 ☐ State legal authority for collecting the SIN:

OR, in the absence of a legal authority to collect the SIN:

3.3 ☐ Establish explicit authority through legislative amendment(s).

3.4 ☐ Establish legal authority as outlined in the *Directive on Social Insurance Number*.

AND, if disclosure of the SIN by the CBSA is to occur on a routine or systematic basis

3.4.1 ☐ To another federal institution that is authorized to collect it, or to another level of government, establish an agreement or arrangement that includes specific provisions to limit the use of the SIN.

3.4.2 ☐ To a contractor or other external service provider, establish a contract that includes specific provisions to limit the use of the SIN.

3.5 ☐ AND, ensure that the relevant **PIB** for the program or activity states the authority under which the SIN is collected and the purpose for which it is used.

NO

3.6 ☒ The SIN is not necessary and it will not be collected, used or disclosed to administer the program or activity.

4. Direct Collection - Notification and Consent (as appropriate)

Is personal information collected directly from the individual to whom it relates?

YES

4.1 ☒ A "**Privacy Notice**" (adapted for either verbal or written communications) must be provided to the individual at the time of collection and it must include the following elements:

a) The purpose and authority for the collection
b) Any uses or disclosures that are consistent with the original purpose.

c) Any uses or disclosures that are not related to the original purpose
d) Any legal or administrative consequences for refusing to provide the personal information
e) That the "individual to whom the information relates" has rights of access to, correction of and protection of personal information under the *Privacy Act*.
f) A reference to the **PIB** for the program or activity
g) Why the SIN is collected, how it will be used and the consequence of not providing it.

AND, add a "**Consent Statement**" to the "**Privacy Notice**" as appropriate, if the personal information is to be used or disclosed for a purpose other than the original purpose (**Secondary Use**) or a consistent use, or, to authorize indirect collection of personal information.

4.2 ☐ The "**Consent Statement**" must include the following elements:

a) The purpose of the consent and the specific personal information involved.
b) In the case of indirect collections, the sources that will be asked to provide the information.
c) Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought.
d) Any consequences that may result from withholding consent.
e) Any alternatives to providing consent

4.3 ☐ AND, implement controls and procedures to ensure that the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

Additional Consent Considerations (s. 77(1)(m) of the *Privacy Act*):

☐ Standards and mechanisms are in place to ensure that the individual has capacity to give consent.

IRCC has taken a several steps to ensure applicants are well notified of the biometric requirement as well as the purpose of collection, namely:

- At a POE, a Privacy Notice is posted on the wall with the LiveScan enrolment device.

NO

4.4 ☐ The personal information necessary for the program or activity is not collected directly from the individual. It is collected indirectly, for example, from another program within the CBSA, or from another institution, government or third party.

5. Indirect Collection - Consent or Authority under Sec. 10 of Privacy Regulations

Is personal information collected indirectly from another source with the informed consent of the individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of the Privacy Regulations?

YES

5.1 ☐ The notice and consent requirements stated at Question 4 apply. Please provide the "**Privacy Notice**" and/or "**Consent Statement**" below:

5.2 ☐ AND, implement controls and procedures to ensure the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

5.3 ☐ AND, if information is being collected from persons authorized to act on behalf of minors, incompetents or individuals who have been deceased for less than 20 years, implement appropriate mechanisms to ensure that such persons are authorized to act on behalf of individuals who do not have the capacity to provide consent.

NO

5.4 ☒

The information collected from the applicant directly; however, there are instances where a person acting on behalf of a minor or a person with a physical limitation to biometric collection can assist. As noted above, Privacy Notices are posted at all sites as required.

6. Indirect Collection - Without Notification and Consent

Is personal information collected from another source without notice to or consent from the individual to whom the information relates?

YES

6.1 ☐ Where information is collected indirectly under any of the following circumstances without notice to, or consent from, the individual to whom it relates, please check the applicable boxes and explain as requested:

☐ a) The collection is a result of a disclosure to the CBSA under subsection 8(2) of the *Privacy Act*. State the applicable paragraph(s) of subsection 8(2) and provide a brief explanation for each:

Details:

☐ b) Direct notification of the individual might result in the collection of inaccurate information, or might defeat the purpose or prejudice the use for which the information is collected. Briefly explain why notice is not provided.

Details:

☐ c) The information involved in the program or activity is to be used solely for a non-administrative purpose in which no decisions are made about the individuals to whom the information relates.

6.2 ☐ AND, if any of the circumstances in a) b) or c) is applicable, ensure that it is reflected in the relevant **PIB**.

6.3 ☐ AND, if the information is to be used solely for a non-administrative purpose (box c above has been checked), ensure that the requirements under sections 6.3.2 and 6.3.3 of the *Directive on Privacy*

Impact Assessment have been met, and that the decision of the official responsible for section 10 of the *Privacy Act* to proceed with a CBSA PIA for the program or activity has been adequately documented in the description of the program or activity in "*Section 1 - Overview and PIA Initiation*" of the CBSA PIA.

6.4 ☐ OR, if none of the circumstances in a) b) or c) is applicable, then the personal information must be collected directly from the individual, or indirectly with the consent of the individual. Please review the responses to Questions 4 and 5 and ensure that the "**Privacy Notice**" or the "**Consent Statement**" includes all of the required elements within Question 4.

NO

6.5 ☒ All personal information is collected directly from the individual to whom it relates, or from another source with notice to, or consent from, the individual or a person authorized to act on behalf of the individual (see Questions 4 and 5 above).

7. Retention and Disposal of Personal Information

Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information?

YES

7.1 ☒ Please identify the Disposition Authorization (DA) and describe the retention and disposal schedule:

7.2 ☒ AND, implement controls and procedures to ensure that personal information used to make a decision that directly affects an individual will be retained for a minimum of two years after the last administrative action or, where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his/her rights under the Act.

7.3 ☒ AND, if the CBSA intends to dispose of personal information that has been used for an administrative purpose prior to the expiration of the two-year minimum retention standard established by the *Privacy Regulations*, it must obtain the consent of the individual to whom the information relates before doing so.

7.4 ☒ AND, the CBSA must cite the DA number, the retention period and the disposition standards for the personal information in the relevant **PIB**.

Details: All CBSA information holdings are governed by Disposition Authorization 2015/008.

Personal information identified in CBSA PPU 1203 will be retained for fifteen years from the time of the most recent biometric collection and will systematically be destroyed after fifteen years or upon granting of Canadian Citizenship. For those persons deemed inadmissible under sections 34-37 of the *Immigration and Refugee Protection Act*, the fingerprints will be retained until the person reaches the age of 100. This has been established to align to the retention period of IRCC (GCMS).

NO

7.5 ☐ Provide a Records Disposition Submission to Library and Archives Canada describing the records containing the personal information for which the institution requires a DA.

7.6 ☐ AND, obtain a DA from Library and Archives Canada to allow the CBSA, under certain conditions, to dispose of records that no longer have operational utility for the program or activity.

7.7 ☐ AND, ensure that all the other applicable requirements listed under "**YES**" at Question 7 are met.

8. Accuracy of Personal Information

Will measures be adopted to ensure that personal information used by the CBSA for an administrative purpose is as accurate, up-to-date and complete as possible?

YES

8.1 Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:

8.1.1 ☒ Personal information will be collected directly from the individual to whom it relates or it will be validated with the individual or a person authorized to act on behalf of the individual.

8.1.2 ☒ A data-matching process will be used to verify the accuracy of personal information against a "reliable source" (within or outside the CBSA) where this is authorized, or where consent was obtained.

8.1.3 ☐ In cases where direct collection or consent is not feasible, the CBSA will obtain information from trusted sources (public or private) and verify accuracy against existing personal information before use.

8.1.4 ☒ Technological methods will be used to identify errors and discrepancies.

8.1.5 ☐ Other

8.2 ☒ AND, if measures are adopted other than "*direct collection or validation with the individual or with a person authorized to act on behalf of the individual*", the CBSA must implement appropriate controls and procedures to ensure that:

a) The technique(s) and the specific source(s) used to validate or update the personal information are documented;

b) Individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them;

c) Personal information can only be modified or corrected by those within the CBSA who have the authority to do so;

d) When personal information is corrected or annotated, the record of personal information indicates the date of the last correction or annotation and the source of the information used to make the correction or annotation; and

d) When personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the CBSA are corrected / annotated.

8.3 ☒ AND, if appropriate, ensure that the "**Privacy Notice**" or "**Consent Statement**" and the relevant **PIB** are amended to identify the data-matching activity including the source(s).

Details:

NO

8.4 ☐

Explain why such measures will not be adopted:

9. Use of Personal Information

Will the personal information collected for the program or activity be used solely for the original purpose for which it was obtained or compiled, a use consistent with that purpose, or a purpose for which the information was disclosed to the institution pursuant to subsection 8(2) of the Privacy Act?

YES

9.1 ☒ Implement controls and procedures to ensure that access to the personal information for such purposes will be limited to authorized individuals who need to know the information to perform their official duties.

Details: Access to the data systems is defined by user profile; users have specific roles based on their job. External to the CBSA, access to the information is limited to other government departments, such as StatsCan, who require the information to fulfil their mandate and with whom the CBSA has an established Memorandum of Understanding or information sharing agreement. Access to the data by all parties would be pursuant to *subsection 8(2) of the Privacy Act*.

9.2 ☒ AND, ensure that the "Data Flow Diagram" or "Data Flow Tables" completed for "*Section 4 – Flow of Personal Information*" of the CBSA PIA identify the areas, groups and individuals (e.g., the positions) within the CBSA who have a need-to-know to access to or handle the personal information, including their geographical location and where the personal information will be stored or retained.

9.3 ☒ AND, if the purposes for which the personal information is used includes any use(s) of the information for a non-administrative purpose, (such as research, statistical, audit and evaluation purposes) the CBSA will adhere to the requirements and principles in the **CBSA *Privacy Protocol For Non-Administrative Purposes*** (2012), in accordance with section 6.2.15 of the *Policy on Privacy Protection*, to address any impact that such non-administrative uses may have on privacy.

NO

9.4 ☐ Identify below any other uses of the personal information, in other words, any routine uses that are not directly related to the purpose of the collection, or, which are not consistent with that purpose or for which the information was disclosed to the CBSA pursuant to subsection 8(2) of the *Privacy Act*:

Detail :

9.5 ☐ AND, ensure that these other uses are reflected in the relevant **PIB**.

9.6 ☐ AND, include a description of these other uses in the "**Privacy Notice**" or "**Consent Statement**", as appropriate,

☐ AND, ensure the all the other applicable requirements listed under "**YES**" at Question 9 are met.

10. Disclosures Directly Related to the Administration of the Program or Activity

Will personal information be disclosed for purposes directly related to the administration of the program or activity?

YES

10.1 ☒ Please check all applicable boxes below and, for each disclosure, identify the name of the organization or third party to which personal information will be disclosed. If it is disclosed within the CBSA, please identify the branch and the program or activity.

10.1.1 ☒ Within the CBSA for another program or activity

Details: The Agency's Inland Enforcement Program may use the information collected for identity management purposes.

10.1.2 ☒ Other federal government institutions

Details: IRCC and the RCMP may use information collected for identity management purposes. IRCC would have access to information in GCMS. RCMP would have access to the fingerprint and Client Identification.

10.1.3 ☐ Provincial, territorial or municipal governments institutions

10.1.4 ☒ Foreign government institutions and entities thereof

Details: Canada may send biometric-based queries to M5 partners from applications made at a POE on a case-by-case basis subject to need and time constraints. Biometric-based queries will be sent to the US for all immigration applications made overseas and at in-Canada service locations. This represents an increase of approximately 2.8 million queries annually over and above the 400,000 queries already taking place under the current program. It is anticipated that the US will send a reciprocal volume of biometric-based queries to Canada.

Biometrics expansion will increase results in automated biometric-based information sharing with each of the M5 partners (Australia, New Zealand and UK). Disclosures of personal information for this purpose would be in accordance with the disclosure provisions of subsection 8(2) of the *Privacy Act*. Canada will query the remaining M5 partners on approximately 400,000 applicants per country per year; a smaller volume of exchanges than with the US. This volume is based on multilateral discussions regarding each country's capacity to send and receive international queries. Determining factors, such as risk and volumes, will be integrated into system rules to establish which queries are sent to each of the M5 partners. In turn, Canada will process an annual total of up to 1.2million requests received from M5 partners (excluding the US). Expanding query-based biometric information sharing to include the remaining M5 partners will allow Canadian officers access to valuable identity and admissibility information on third country nationals held by the immigration authorities of those countries.

10.1.5 ☐ International organizations

10.1.6 ☐ The private sector (e.g., contractor or other external service provider)

10.1.7 ☐ Other

10.2 ☒ AND, ensure that:

a) any such disclosure is made in compliance with section 8 of the *Privacy Act*, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act;

b) only personal information elements that are necessary for the intended purpose are disclosed;

c) the organization or third party receiving the personal information is authorized to do so;

d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see Question 15);

e) the organization or third party to which the personal information will be disclosed for the administration of the program or activity are identified in the "Consistent Use" section in the relevant **PIB** in *CBSA Info Source*, including the specific purpose of the disclosure;

the "**Privacy Notice**" or "**Consent Statement**" describes any disclosures of information;

f) the "Data Flow Diagram" or "Data Flow Tables" completed in "*Section 4 – Flow of Personal Information*" of the CBSA PIA include details on the disclosed personal information:

10.3 ☒ AND, any disclosure of personal information to another federal institution or outside the Government of Canada is governed by a formal agreement or arrangement (e.g., a Memorandum of Understanding, an accord, a contractual arrangement, etc.) to ensure that appropriate privacy protection clauses are included, and, where applicable, include provisions for inter-jurisdictional or transborder flows of personal information. Such clauses must cover the following topics:

a) Control over personal information, where appropriate.

b) Limitations on the collection, retention, use and disclosure of personal information.

c) Measures (administrative, technical and physical) to protect the integrity and confidentiality of personal information.

d) Measures governing the disposition of the personal information, where relevant

e) Measures to ensure or verify that the personal information is only used for the purposes related to the agreement, arrangement or contract.

f) Obligations are to be extended to other parties such as subcontractors.

Details: M5 Immigration Information Sharing has been addressed in the IIS PIA and is conducted under the authority of the following MoU's.

1. Memorandum of Understanding Between The Department of Citizenship and Immigration of Canada and the Canada Border Services Agency and The Department of Immigration and Border Protection of the Commonwealth of Australia Regarding the Exchange of Information (MoU)
   A) Annex to the MoU Concerning the Exchange of Information on a Case-by-Case Basis
   B) Annex to the MoU Concerning the Exchange of Information on an Automated Basis
2. Memorandum of Arrangement Between The Department of Citizenship and Immigration of Canada and the Canada Border Services Agency and The New Zealand Ministry of Business, Innovation and Employment (Immigration New Zealand) Regarding the Exchange of Information (MoA)
   A) Annex to the MoA Concerning the Exchange of Information on a Case-by-Case Basis
3. Memorandum of Understanding Between the Department of Citizenship and Immigration of Canada and the Canada Border Services Agency and the United Kingdom Secretary of State for the Home Department Acting Through the Home Office Regarding the Exchange of Information
   A) Annex to the MoU Concerning the Exchanger of Information on a Case-by-Case Basis
4. Implementing Arrangement Between the Department of Citizenship and Immigration of Canada and the Canada Border Services Agency, on the One Side and the Department of State and the Department of Homeland Security of the United States of America, on the Other Side, Concerning Biometric Visa and Immigration Information Sharing

NO

10.4 ☐ There is no disclosure of personal information within or outside the institution for purposes that are directly related to the administration of the program or activity.

11. Accounting for New Uses or Disclosures Not Reported in CBSA Info Source

Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant PIB published in CBSA Info Source?

YES

11.1 ☒ Appropriate controls and procedures have been or will be implemented to ensure that:

a) the head of the institution (The ATI and Privacy Director) or the appropriate delegate is notified about any new use or disclosure of personal information that is not reflected in the **PIB** description published in *CBSA Info Source*;

b) the consent of the individual to whom the information relates is obtained in writing, as appropriate, prior to any new use of the information for an administrative purpose that is not reflected in the relevant **PIB** published in *CBSA Info Source*, unless the new use is considered to be consistent with the purpose for which the personal information was obtained or compiled and the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith regarding the new consistent use;

c) except as permitted under subsection 8(2) of the *Privacy Act*, any disclosure of personal information for a purpose that is not reflected in the relevant **PIB** published in *CBSA Info Source* will only be made with the consent of the individual to whom the information relates;

d) a record is kept for any new use or disclosure of personal information not described in the relevant **PIB** published in *CBSA Info Source,* and that this record is stored with the personal information to which it relates and retained for a minimum period of two years following such a use or disclosure;

e) if the information is disclosed to a federal investigative body under paragraph 8(2)(e) of the *Privacy Act*, the record of disclosure will be kept in a separate PIB for a period of two years where it will be available to the Privacy Commissioner for review upon request;

f) the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith, as required under subsection 9(4) of the Act, of any new use or disclosure that is consistent with the purpose for which the information was obtained or complied, but which is not reflected in the relevant **PIB** published in *CBSA Info Source*;

g) the relevant **PIB** is amended in time for the next edition of *CBSA Info Source* to include any new use(s) or disclosure(s) that are consistent with the purpose for which the information was obtained or compiled, as well as any routine use(s) or disclosure(s) that do not fall within the categories of purpose of collection or consistent use; and

h) the Privacy Commissioner is notified, by the ATI and Privacy Director, prior to or forthwith, as required under subsection 8(5) of the Act, about any disclosures made or to be made in the public interest or in the interest of the individual to whom the information relates.

i) Other

NO

11.2 ☐ Please explain why such controls and procedures will not be implemented

Detail:

12. Safeguards - Statement of Sensitivity

Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of the personal information to be collected and retained for the program or activity?

YES

12.1 ☒ The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "*Section 2 - Risk Area Identification and Categorization*" of the CBSA PIA.

Details: A Statement of Sensitivity (SoS) has been completed for the TRBP. As the information collected under TRBP is identical with the expanded population, the TRBP SoS is still applicable.

NO

12.2 ☐ Please explain why a SoS or similar analysis was not considered necessary to assess the sensitivity of the information.

13. Safeguards - Threat and Risk Assessment

Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the program or activity?

YES

13.1 ☐ Reference the title of the TRA or other security assessment in "*Section 6 – Supplementary Documents List*" and provide a brief synopsis of the assessment in the space below:

Details :

13.2 ☐ AND, obtain assurances from the officials responsible for the program or activity that the measures recommended in the assessment have been implemented to ensure the confidentiality, availability and integrity of the personal information.

13.3 ☐ AND, ensure that any residual risks to personal information are known and accepted by the executive or senior official responsible for the program or activity and the Head or delegated authority for the *Privacy Act*. (ATI and Privacy Director)

NO

13.4 ☒ If a TRA or similar security assessment is underway, simply reference that fact in the space below and indicate when it is likely to be completed. If there is no intent to complete one, please explain.

Details: A CSAR has been prepared for the Biometrics Expansion Project. The CSAR, as per standard project process, is reviewed and revised as the project progresses and will be finalized prior to coming-into-force on July 31, 2018.
The potential risks created by the timing of the CSAR in the project process - Service Lifecycle Management Framework (SLMF) – will be raised with the CBSA Management.

14. Safeguards - Administrative, Physical and Technical

Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this program or activity to ensure the confidentiality, availability and integrity of the personal information.

Please check all that apply, including safeguards identified by the TRA or similar security assessment.

14.1 Administrative safeguards

- ☒ Internal security and privacy policies and procedures
- ☒ Staff training on privacy and the protection of personal information
- ☒ Screening and security checks of employees
- ☒ Appropriate security levels for employees who will have access to personal information
- ☒ Contingency plans and documented procedures in place to identify and respond to security and privacy breaches, and to communicate security violations to the data subject, law enforcement authorities and relevant program managers
- ☒ Regular monitoring of users' security practices
- ☒ Methods to ensure that only authorized personnel who need to know have access to personal information
- ☐ Other

Details:

14.2 Physical safeguards

- ☒ Restricted access areas
- ☒ Security guards
- ☒ Identification badges are worn by staff at all times
- ☒ After hours alarms and monitoring systems
- ☒ Locked filing cabinets
- ☒ Combination locks
- ☒ Video surveillance (closed-circuit television)
- ☒ Secured server locations
- ☒ Backups secured off-site
- ☐ Other

Details:

14.3 Technical safeguards

- ☒ Role-based user authorization and authentication
- ☒ Passwords (minimum of 6 characters long, include alpha and numeric characters)
- ☒ Passwords are changed by users every 90 days and recently used passwords cannot be re-used)

- ☒ Password protected screensavers
- ☒ Session-time out security (automatically locks an account after a session has been idle for a specified amount of time)
- ☒ Firewalls
- ☒ Virtual Private Network (VPN)
- ☐ Encryption of sensitive information
- ☐ Government of Canada Public Key Infrastructure Certificates (PKI)
- ☒ External Certificate Authority (CA)
- ☒ Audit trails
- ☐ Other

Details:

15. Technology and Privacy - Tracking Technologies

Will the information system(s) used to deliver the program or activity employ cookies or other tracking technologies to collect personal information about users and their transactions?

YES

15.1 ☐ The specific tracking technologies to be used is adequately described under Part 6: Technology and Privacy of "*Section 2 – Risk Area Identification and Categorization*" of the CBSA PIA;

15.2 ☐ AND, the collection of any personal information using such technologies is reflected in the relevant **PIB** and in "*Section 3 – Analysis of Personal Information Elements*" of the CBSA PIA;

15.3 ☐ AND, the use of such technologies to collect information about users and their transactions is adequately reflected in the "**Privacy Notice**";

15.4 ☐ AND, those responsible for implementing and using tracking technologies to collect personal information or who may have access to personal information collected through these methods are made aware of privacy and security policy requirements;

15.5 ☐ AND, where personal information collected through such tracking technologies is used to make a decision that directly affects the individual to whom the information relates, it will be retained for a minimum of two years after the last administrative action as required under the *Privacy Regulations*.

NO

15.6 ☒ Tracking technologies are not used to collect personal information about users.

16. Technology and Privacy - Surveillance or Monitoring

Will the new or modified program or activity result in new or increased surveillance or monitoring of a targeted population?

YES

16.1 ☐ Consult with your legal advisors to determine whether or not such surveillance or monitoring activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.

16.2 ☐ And, ensure the surveillance or monitoring method(s) to be used, the characteristic(s) of the targeted population and the scope of the surveillance or monitoring are adequately described under Part 6: Technology and Privacy of "*Section 2 – Risk Area Identification and Categorization*" of the CBSA PIA.

16.3 ☐ AND, any personal information collected or created as a result of such surveillance or monitoring is described in the relevant **PIB** and in *Section 3 – Analysis of Personal Information Elements*" of the CBSA PIA.

16.4 ☐ AND, the collection or use of personal information through surveillance or monitoring is adequately reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the personal information is collected.

☐ If notice about surveillance or monitoring will not be provided

Detail explain why:

16.5 ☐ AND, those responsible for implementing and using such surveillance or monitoring method(s) or who may have access to personal information collected or created through these methods are made aware of privacy and security policy requirements.

NO

16.6 ☒ The new or modified program or activity will not result in additional surveillance or monitoring.

17. Considerations Related to Compliance, Regulatory Investigation, Enforcement

Does the program or activity involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?

YES

17.1 ☒ Consult with your legal advisors to determine whether or not the compliance/regulatory investigation or law enforcement activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.

17.2 ☒ AND, identify the legislative authority and the specific regulatory or law enforcement purpose involved:

Details: The IRPA and subsequent IRPR provide the authority to collect biometric information as well as the circumstances in which a person is require to provide their biometric information for the purposes of identification and determination of admissibility of the person. Failure to comply with an obligation or requirement specified in the Act or Regulations could result in a finding on inadmissibility under the IRPA, or in some cases, criminal charges as a result of a violation of the IRPA.

Immigration and Refugee Protection Act (S.C. 2001, c. 27) states:

- 10.01 A person who makes a claim, application or request under this Act must follow the procedures set out in the regulations for the collection and verification of biometric information, including procedures for the collection of further biometric information for verification purposes after a person's claim, application or request is allowed or accepted.

Obligation — answer truthfully

- 16 (1) A person who makes an application must answer truthfully all questions put to them for the purpose of the examination and must produce a visa and all relevant evidence and documents that the officer reasonably requires.
- Marginal note: Obligation — appear for examination

  (1.1) A person who makes an application must, on request of an officer, appear for an examination.
- Marginal note: Obligation — relevant evidence

  (2) In the case of a foreign national,
  - (a) The relevant evidence referred to in subsection (1) includes photographic and fingerprint evidence; and
  - (b) Subject to the regulations, the foreign national must submit to a medical examination.
- Marginal note: Obligation — interview

  (2.1) A foreign national who makes an application must, on request of an officer, appear for an interview for the purpose of an investigation conducted by the Canadian Security Intelligence Service under section 15 of the Canadian Security Intelligence Service Act for the purpose of providing advice or information to the Minister under section 14 of that Act and must answer truthfully all questions put to them during the interview.
- Marginal note: Evidence relating to identity

  (3) An officer may require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence — photographic, fingerprint or otherwise — that may be used to establish their identity or compliance with this Act.
- 2001, c. 27, s. 16;
- 2010, c. 8, s. 2;
- 2013, c. 16, s. 5;
- 2015, c. 3, s. 108(E).
- 124 (1) Every person commits an offence who

  (a) contravenes a provision of this Act for which a penalty is not specifically provided or fails to comply with a condition or obligation imposed under this Act.

17.3 ☒ AND, if the legislative authority differs from the legal authority for the program or activity, ensure it is adequately reflected in the response to Question 1 of *"Section 5 – Privacy Compliance Analysis"* and in *"Section 1 – Overview and PIA Initiation "*of the CBSA PIA.

17.4 ☒ AND, any personal information collected or created as a result of such regulatory or criminal enforcement, surveillance or intelligence gathering program or activity is described in the relevant **PIB** and in *"Section 3 – Analysis of Personal Information Elements"* of the CBSA PIA.

17.5 ☒ AND, the collection or use of personal information through these compliance / regulatory investigation or enforcement activities is adequately reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose, or prejudice the use, for which the personal information is collected.

Details: A Privacy Notice, which will be updated upon final publication of support regulations is posted on the wall at each LiveScan device where it will be visible at the beginning of the biometric enrolment.

Privacy Notice

To individuals who are required to submit fingerprints and photographs under the *Immigration and Refugee Protection Act*:

Legislative authority to fingerprint:

Where fingerprints and photographs of applicants seeking admission into Canada are requested, compliance is required by law. Failure to comply may result in inadmissibility. The legal authority to collect this personal information are sections 10.01 and 16 of the *Immigration and Refugee Protection Act*.

Purpose of the collection of fingerprints:

The personal information you are required to provide will be used to assess your application in accordance with the *Immigration and Refugee Protection Act*. The information may be shared with other law enforcement agencies in accordance with the *Privacy Act*.

Retention and disposal standards:

Paper records are normally retained ten years after the last administrative action. RDA Number: 90/002 Related to PR# CIC ASB 001. TBS Registration: 005218 Bank Number CIC PPU 001 (formerly EIC PPU 270).

Access to personal information:

Under the *Privacy Act* and the *Access to Information Act*, individuals have the right to protection and access to their personal information. Details on these matters are available at www.infosource.gc.ca and through the IRCC Call Centre. Info Source is also available in Canadian public libraries. For further information contact:

Immigration, Refugees and Citizenship Canada

Access to Information and Privacy Coordinator

Public Rights Administrator Division

Narono Building

360 Laurier Avenue, 10th floor

☐ If notice about the compliance/regulatory investigation or law enforcement activities will not be provided.

NO

17.6 ☐ The program or activity does not involve the conduct of regulatory or criminal enforcement, surveillance or intelligence gathering.

SECTION 6 - Summary of Analysis and Recommendations

This table summarizes the privacy risks identified through the PIA process, and categorizes levels of risk as low, moderate, or high. Risk is defined by factors of impact and likelihood of occurrence. The goal of privacy risk management is to maintain privacy risks within acceptable bounds. The higher ratings provide an indication of priority areas for implementing suggested risk mitigation mechanisms. Criteria for ranking are set as follows:

(L)ow: There is a remote possibility that the risk will materialize and/or the impact of the risk to the program is minor.
(M)oderate: The possibility of the risk materializing is very low although the impact of such a risk is high, *OR* the possibility of the risk materializing is high but the impact of such a risk is minor, *OR* the impact and likelihood of the risk occurring are both determined to be moderate.
(H)igh: There is a near certainty that the risk will materialize if no corrective measures are taken and/or the impact of the risk on the program is severe.

Element	Nature of Risk	L	M	H	Recommendations
Retention and Disposal of Personal Information	CBSA retention period for data collected via traveller processing varies by initiative, from 7 years to 15 years.		x		CBSA to conduct a review of the retention period for information collected via traveller processing, and explore the possibility of aligning the traveller processing records for entry, which are currently retained for seven years, with the retention period for Entry/Exit initiative (exit records), which is set for 15 years retention past the point of collection.
Future Border Processing	A PIA has not been conducted.		x		A PIA be completed for the Generic Passage Flow (GPF) initiative. This initiative will enable a unified operational model with tightly integrated and standardized business processes, information and technology that are used throughout the border processing continuum and includes people, goods, or conveyances in all modes, pre-border, at the border, post border, and applies to all CBSA programs. The project goal is to provide one process and one system for the traveller passage continuum.

Primary Processing	A PIA has not been conducted.		x		The Agency has not conducted a PIA on general primary processing; as such, the risks are unknown at this time.
A PIB related specifically to Biometrics	A new PIB had been approved in principle for the Biometrics Expansion Project, but has yet to receive formal approval and has not yet been published. The PIB is attached to this assessment.		x		The PIB for the Biometrics Expansion Program has been created and required formal approval from TBS for publication.

SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST

List of supplementary documents that support the conclusions of this CBSA Privacy Impact Assessment. For each document, the specific sections of the documents (subject, chapter, page, paragraph, etc.) that correspond with the CBSA PIA are cited and linked to the PIA sections.

Document	Document Reference	PIA Reference
RCMP/CBSA Service Level Agreement (SLA)	Entire SLA	Section 2 Risks p.21
Information Sharing Toolkit: 1. Policy on Disclosure of Personal Information: Section 8 of the *Privacy Act* 2. Policy on the Disclosure of Customs Information: Section 107 of the *Customs Act* 3. Directive on Sharing Information Pursuant to the *Security of Canada Information Sharing Act* (SCISA) 4. Policy on Implementing the Ministerial Direction to the CBSA on Information Sharing with Foreign Entities 5. Operational Guidelines on the Ministerial Direction 6. Public Interest Disclosures under 8(2)(m)(i) of the *Privacy Act* 7. Public Interest Disclosures under s. 107(6)(a) of the *Customs Act* 8. Operational Guidelines on the Disclosure of Information for Enforcement and Intelligence 9. CBSA Information Sharing Checklist 10. FAQs relating to the *Privacy Act* and the *Customs Act*	Entire toolkit	
Operational Bulletin PRG 2018-29: Expansion of the Biometrics Program Coming into Force 1	Entire Document	
CBSA Enforcement Manual Part 7, Chapter 3 (Information Sharing Policy of the Enforcement Program)	Entire Document	
Operational Guidelines - Disclosure of Information for Enforcement and Intelligence	Entire Document	
Biometrics Expansion Project PIB	Draft PIB	Section 6- Analysis

SECTION 8 - FORMAL APPROVAL

The following signature represents a commitment to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements outlined in the CBSA PIA as they relate to the administration of the identified program or activity.

Martin Bolduc, Vice President, Programs Branch

JUL 3 1 2018

Date

Note: Responsibility for sections 4 to 8 of the *Privacy Act* rests with all employees of government institutions that handle personal information. Officials who manage such programs and activities are responsible for ensuring that such requirements are implemented as part of the administration of the program or activity.

The following signature represents a commitment by the Head of the institution or his/her delegate(s) who is responsible for establishing personal information banks in accordance with section 10 of the *Privacy Act*.

Dan Proulx, Director, Access to Information and Privacy Division

JUL 2 5 2018

Date

Note: Under the *Privacy Act*, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks

Annex A: Privacy Compliance Checklist and Other Considerations

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of *Section 5 – Privacy Compliance Analysis*)	Done	To be done
1	Legal authority for the program or activity has been established and is reflected in the relevant PIB.	☒	☐
2	a) The categories and elements of personal information to be collected for the new program or activity have been carefully assessed based, for example, on the CBSA's experience gained with the administration of a similar program or activity. The personal data collected will be limited to only that which is required.)	☒	☐
	b) Categories and elements of personal information have been described in the relevant PIB for the program or activity.	☒	☐
	c) Controls and procedures will be implemented to ensure the CBSA does not collect more personal information than necessary for the program or activity and that a continuing need exists for the personal information and its collection.	☒	☐
4 and 5	a) All of the requisite "Privacy Notices" and "Consent Statements" that meet the requirements of sections 6.2.9 to 6.2.12 of the *Directive on Privacy Practices* have been drafted. (Texts of the notices and consent statements must be included as an annex.)	☒	☐
	b) Controls and procedures have been implemented to keep records of individual consents, and to ensure that persons acting on behalf of individuals who do not have the capacity to provide consent have the authority to do so under section 10 of the *Privacy Regulations*.	☒	☐
7	a) A Disposition Authorization (DA) has been approved by Library and Archives Canada to authorize the disposal of the records containing personal information for the program.	☒	☐
	b) Controls and procedures have been implemented within the program or activity and the CBSA ATI and Privacy Division to ensure that information that has been used for an administrative purpose will be kept for the minimum retention period established by the *Privacy Regulations*.	☒	☐
	c) Reference to the DA, the retention period and the disposition standards for the program have been cited in the relevant PIB.	☒	☐
8	Controls and procedures are in the process of being implemented to ensure that the personal information associated with the program is as accurate, complete and up-to-date as necessary.	☒	☐

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of *Section 5 – Privacy Compliance Analysis*)	Done	To be done
Other Privacy Considerations related to specific principles that are not explored in the previous 17 sections: (these considerations should be explored in the Executive Summary)			
Openness	Describe how the results of any privacy impact assessment or audit will be made available to the public. The Executive Summary will be published on the external CBSA ATI and Privacy Division website at http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pias-sefp-eng.html	☐	☒
	Are policies and practices relating to the proposal's management and handling of personal information available to the public?	☒	☐
	Is there a communications plan to explain to the public how personal information will be managed and protected?	☒	☐
	Is there a clearly defined and easy process for individuals to access such information and/or communicate with appropriate individuals with respect to policies and practices relating to management and protection of personal information?	☒	☐
	Where appropriate, will public consultation take place on the privacy implications of the proposal?	☒	☐
Individual's Access to Personal Information	Is the system designed to ensure that an individual can have access to his/her personal information, including all other programs or applications that have received copies of the information? s. 12(1)	☒	☐
	Are there documented procedures developed or planned on how to make privacy requests or requests for the correction of personal information? s. 12 (2)	☒	☐
	Are individuals provided with access to their personal information in the official language of their choice? s. 17(2)	☒	☐
	If appropriate, are individuals provided with access to their personal information in an alternative format? s. 17(3)	☒	☐
Challenging Compliance	Are the complaint procedures for the proposed program or service consistent with legislated requirements? s. 29-35	☒	☐
	To improve information management practices and standards, has a procedure been established to log and periodically review the nature, frequency and resolution of complaints?	☒	☐
	Are there oversight and review mechanisms implemented or available to ensure accountability?	☒	☐

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of *Section 5 – Privacy Compliance Analysis*)	Done	To be done
	Have oversight agencies, including the Office of the Privacy Commissioner, issued reports or opinions on issues that would be relevant to the proposal?	☒	☐